IN THE CLAIMS:

Please amend claims 3, 5, 6, 9, 11-13, 15, 16, 19, 21, 22, 25, 27-29, 31, 32, 35, 37, 38, 41, 43-45, 47, and 48 as follows.

1. (Original) A method for requesting a digital certificate in a mobile telecommunications network, the method including the steps of:

sending a request for a digital certificate from a subscriber to a network element via the network, the request including a first part and a second part;

wherein the first part is sent via an authenticated communication channel of the network and the second part is sent via an unprotected communication channel of the network.

2. (Original) A method according to claim 1, wherein the first part includes data that is relatively more security-critical than data in the second part.

3. (Currently Amended) A method according to claim 1 ~~or 2~~, further including the steps of:

sending a response to the request, the response including a third part and a fourth part;

wherein the third part is sent via an authenticated communication channel of the network and the fourth part is sent via an unprotected communication channel of the network.

4. (Original) A method according to claim 3, wherein the third part includes data that is relatively more security-critical than data in the fourth part.

5. (Currently Amended) A method according to ~~any one of the preceding claims~~ claim 1, wherein:

the authenticated channel is a signaling plane; and

the unprotected channel is a user plane.

6. (Currently Amended) A method according to ~~any one of the preceding claims~~ claim 1, wherein the first part includes a cryptographic hash of the public key of the subscriber.

7. (Original) A method according to claim 6, wherein the third part includes a continuation address, and the second part is sent to the continuation address and includes the public key of the subscriber.

8. (Original) A method according to claim 7, wherein the first and second parts are securely linked by checking that the hash received in the first part matches the public key received in the second part.

9. (Currently Amended) A method according to ~~any one of claims 6 to 8~~ claim 6, wherein the fourth part includes a subscriber certificate for the public key issued by an operator certification authority.

10. (Original) A method according to claim 9, wherein the first and second parts are securely linked by checking that the hash received in the first part matches the subscriber certificate received in the second part.

11. (Currently Amended) A method according to ~~any one of claims 6 to 8~~ claim 6, wherein the fourth part contains a further continuation address which triggers a further exchange of one or more rounds of request and response messages, the final of these

messages containing a certificate for the public key of the subscriber issued by the operator certification authority.

12. (Currently Amended) A method according to claim 6 ~~or 7~~, wherein the subscriber's public key is sent after the second part is transmitted, at a time determined by the operator certification authority.

13. (Currently Amended) A method according to ~~any one of claims 1 to 4~~ claim 3, wherein the fourth part includes a certificate of the public key of the operator certification authority or the public key of the operator certification authority.

14. (Original) A method according to claim 13, wherein the third part includes a cryptographic hash of the certificate or public key of the operator certification authority, the third and fourth parts being securely linked by checking that the hash received in the third part matches the certificate or public key received in the fourth part.

15. (Currently Amended) A method according to ~~any one of the preceding claims~~ claim 3, wherein the first and/or third parts include additional security-critical data.

16. (Currently Amended) A method according to ~~any one of the preceding claims~~ claim 3, wherein the second and/or fourth parts include additional non security-critical data.

17. (Original) Communication network apparatus for processing a request for a digital certificate in a mobile telecommunications network, the apparatus being configured to:

receive at a network element a request for a digital certificate from a subscriber, the request including a first part and a second part;

wherein the first part is sent via an authenticated communication channel of the network and the second part is sent via an unprotected communication channel of the network.

18. (Original) Communication network apparatus according to claim 17, wherein the first part includes data that is relatively more security-critical than data in the second part.

19. (Currently Amended) Communication network apparatus according to claim 17 ~~or 18~~, further including the steps of:

sending a response to the request, the response including a third part and a fourth part;

wherein the third part is sent via an authenticated communication channel of the network and the fourth part is sent via an unprotected communication channel of the network.

20. (Original) Communication network apparatus according to claim 19, wherein the third part includes data that is relatively more security-critical than data in the fourth part.

21. (Currently Amended) Communication network apparatus according to ~~any one of claims 17 to 20~~ claim 17, wherein:

the authenticated channel is a signaling plane; and

the unprotected channel is a user plane.

22. (Currently Amended) Communication network apparatus according to ~~any one of claims 17 to 21~~ claim 17, wherein the first part includes a cryptographic hash of the public key of the subscriber.

23. (Original) Communication network apparatus according to claim 22, wherein the third part includes a continuation address, and the second part is sent to the continuation address and includes the public key of the subscriber.

24. (Original) Communication network apparatus according to claim 23, wherein the first and second parts are securely linked by checking that the hash received in the first part matches the public key received in the second part.

25. (Currently Amended) Communication network apparatus according to ~~any one of claims 6 to 8~~ claim 6, wherein the fourth part includes a subscriber certificate for the public key issued by an operator certification authority.

26. (Original) Communication network apparatus according to claim 25, wherein the first and second parts are securely linked by checking that the hash received in the first part matches the subscriber certificate received in the second part.

27. (Currently Amended) Communication network apparatus according to ~~any one of claims 22 to 24~~ claim 22, wherein the fourth part contains a further continuation address which triggers a further exchange of one or more rounds of request and response messages, the final of these messages containing a certificate for the public key of the subscriber issued by the operator certification authority.

28. (Currently Amended) Communication network apparatus according to claim 22 ~~or 23~~, wherein the subscriber's public key is sent after the second part is transmitted, at a time determined by the operator certification authority.

29. (Currently Amended) Communication network apparatus according to ~~any one of claims 17 to 20,~~ claim 19, wherein the fourth part includes a certificate of the public key of the operator certification authority or the public key of the operator certification authority.

30. (Original) Communication network apparatus according to claim 29, wherein the third part includes a cryptographic hash of the certificate or public key of the operator certification authority, the third and fourth parts being securely linked by checking that the hash received in the third part matches the certificate or public key received in the fourth part.

31. (Currently Amended) Communication network apparatus according to ~~any one of claims 17 to 30~~ claim 19, wherein the first and/or third parts include additional security-critical data.

32. (Currently Amended) Communication network apparatus according to ~~any one of claims 17 to 31~~ claim 19, wherein the second and/or fourth parts include additional non security-critical data.

33. (Original) Mobile user equipment (UE) for requesting a digital certificate from a network entity in a mobile telecommunications network, the UE being configured to:

send a request for a digital certificate to the network element via the network, the request including a first part and a second part;

wherein the first part is sent via an authenticated communication channel of the network and the second part is sent via an unprotected communication channel of the network.

34. (Original) Mobile user equipment according to claim 33, wherein the first part includes data that is relatively more security-critical than data in the second part.

35. (Currently Amended) Mobile user equipment according to claim 33 ~~or 34~~, being configured to:

receive a response to the request, the response including a third part and a fourth part;

wherein the third part is received via an authenticated communication channel of the network and the fourth part is received via an unprotected communication channel of the network.

36. (Original) Mobile user equipment according to claim 35, wherein the third part includes data that is relatively more security-critical than data in the fourth part.

37. (Currently Amended) Mobile user equipment according to ~~any one of claims 33 to 36~~ claim 33, wherein:

the authenticated channel is a signaling plane; and

the unprotected channel is a user plane.

38. (Currently Amended) Mobile user equipment according to ~~any one of claims 33 to 37~~ claim 35, wherein the first part includes a cryptographic hash of the public key of the subscriber.

39. (Original) Mobile user equipment according to claim 38, wherein the third part includes a continuation address, and the second part is sent to the continuation address and includes the public key of the subscriber.

40. (Original) Mobile user equipment according to claim 39, wherein the first and second parts are securely linked by checking that the hash received in the first part matches the public key received in the second part.

41. (Currently Amended) Mobile user equipment according to ~~any one of claims 38 to 40~~ claim 38, wherein the fourth part includes a subscriber certificate for the public key issued by an operator certification authority.

42. (Original) Mobile user equipment according to claim 41, wherein the first and second parts are securely linked within the network by checking that the hash received in the first part matches the subscriber certificate received in the second part.

43. (Currently Amended) Mobile user equipment according to ~~any one of claims 38 to 40~~ claim 38, wherein the fourth part contains a further continuation address which triggers a further exchange of one or more rounds of request and response messages, the final of these messages containing a certificate for the public key of the subscriber issued by the operator certification authority.

44. (Currently Amended) Mobile user equipment according to claim 38 ~~or 39~~, wherein the subscriber's public key is received after the second part is transmitted, at a time determined by the operator certification authority.

45. (Currently Amended) Mobile user equipment according to ~~any one of claims 33 to 36,~~ claim 35, wherein the fourth part includes a certificate of the public key of the operator certification authority or the public key of the operator certification authority.

46. (Original) Mobile user equipment according to claim 45, wherein the third part includes a cryptographic hash of the certificate or public key of the operator certification authority, the third and fourth parts being securely linked by checking that the hash received in the third part matches the certificate or public key received in the fourth part.

47. (Currently Amended) Mobile user equipment according to ~~any one of claims 33 to 46~~ claim 35, wherein the first and/or third parts include additional security-critical data.

48. (Currently Amended) Mobile user equipment according to ~~any one of claims 33 to 47~~ claim 35, wherein the second and/or fourth parts include additional non security-critical data.